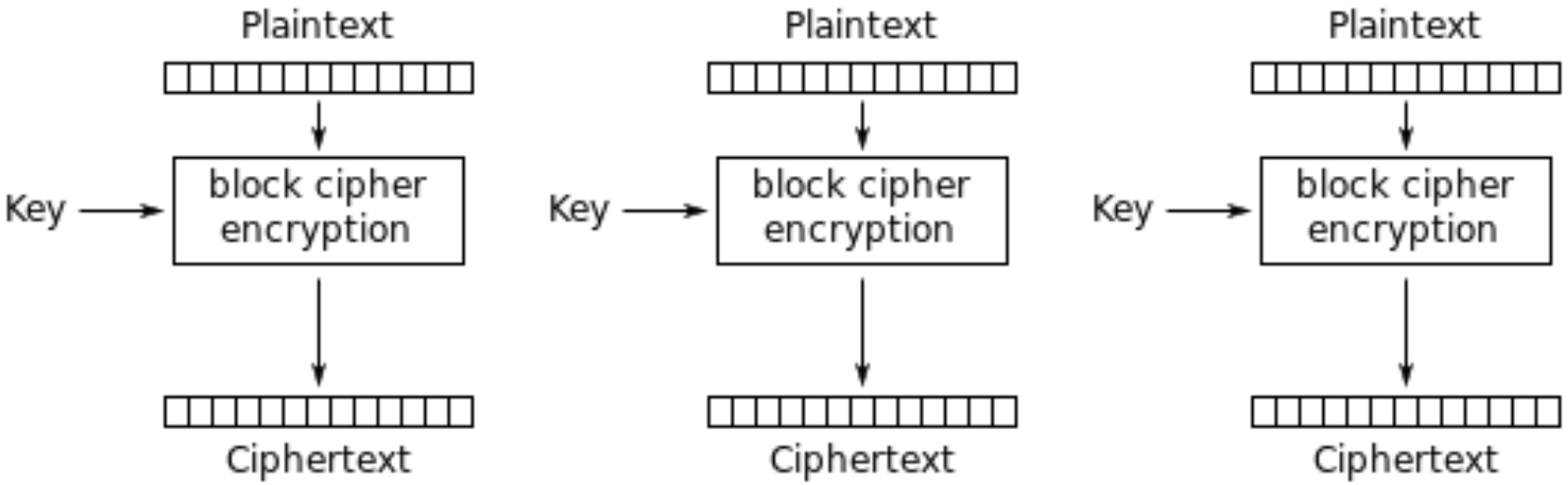
# Режимы шифрования

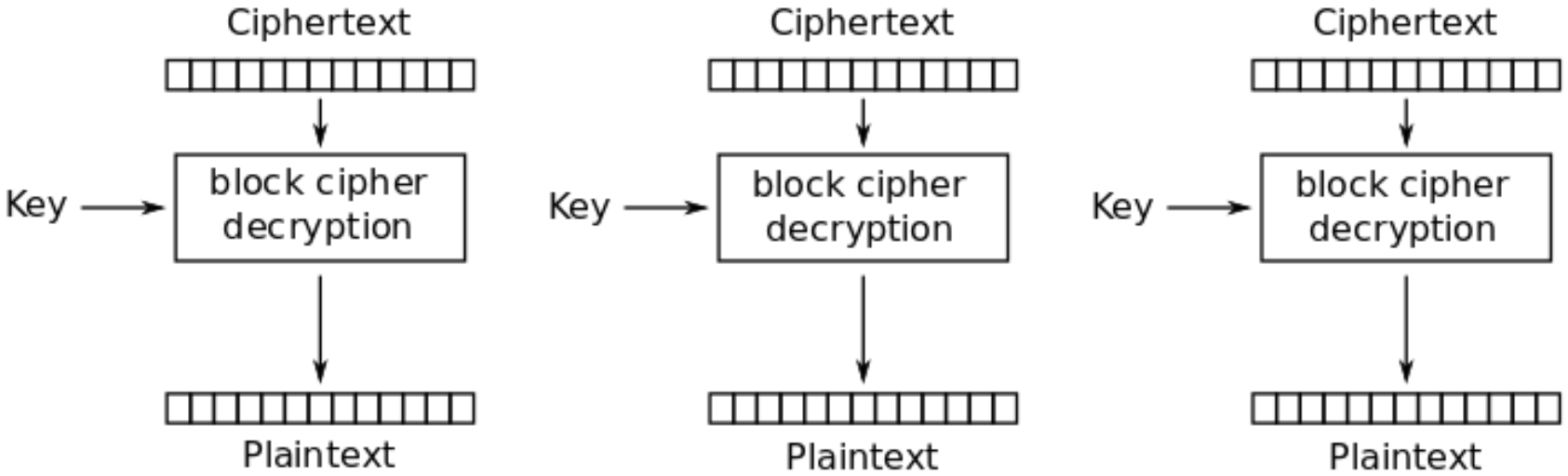
- ECB (простая замена)
- CBC (сцепление блоков шифртекста)
- CFB (гаммирование с обратной связью по шифртексту)
- OFB (гаммирование с внутренней обратной связью)
- Имитовставка

# Режим шифрования ECB. Зашифрование




Electronic Codebook (ECB) mode encryption

# Режим шифрования ECB. Расшифрование

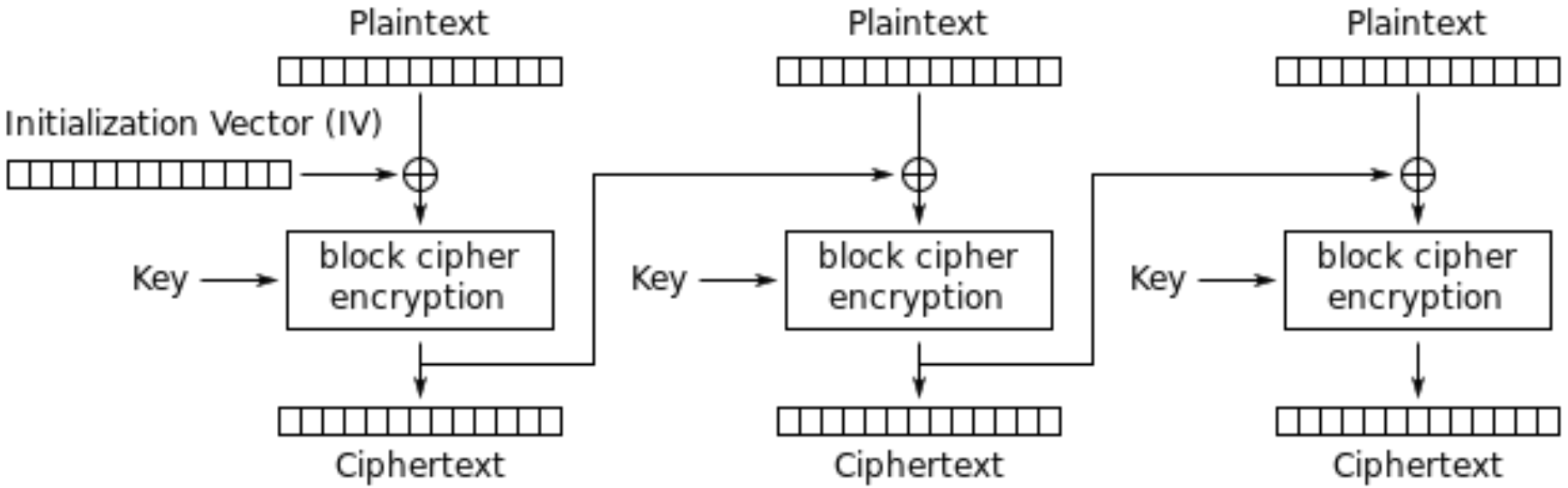



Electronic Codebook (ECB) mode decryption

# Режим шифрования ECB. Свойства

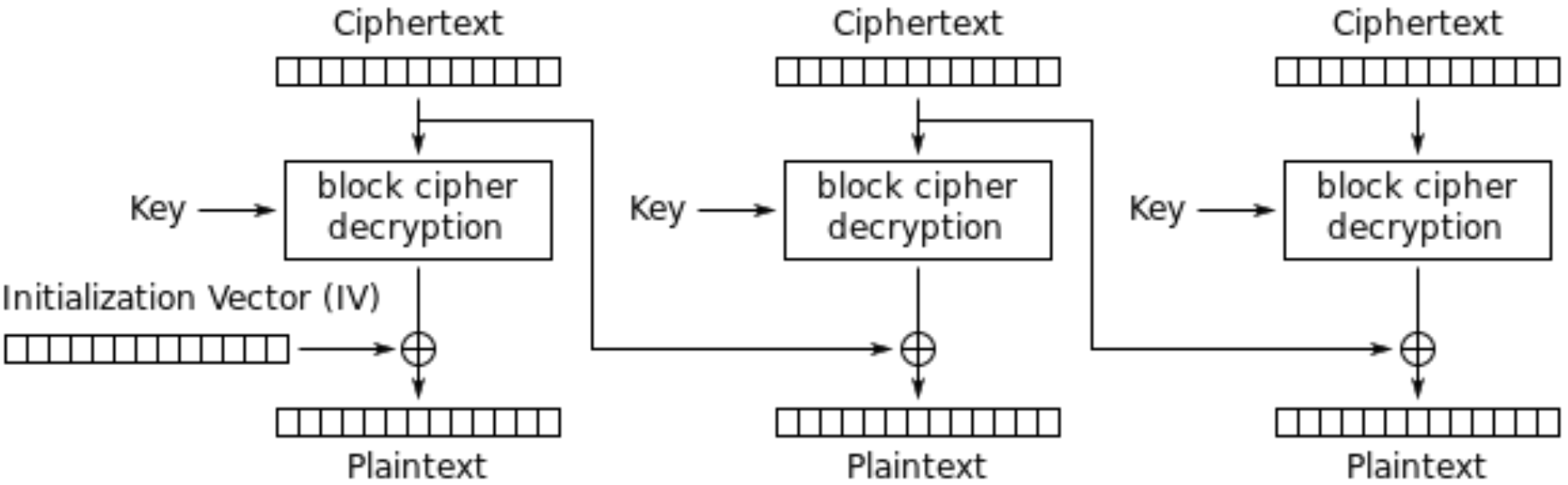
- 1 ошибка в шифртексте ведет к неверному расшифрованию блока. На другие блоки расшифрованного текста ошибка не распространяется
- Одинаковые блоки открытого текста переходят в одинаковые блоки шифртекста
- Нет стойкости к ошибкам синхронизации
- Режим подходит для шифрования коротких сообщений без шаблонов

# Режим шифрования CBC. Зашифрование




Cipher Block Chaining (CBC) mode encryption

# Режим шифрования CBC. Расшифрование

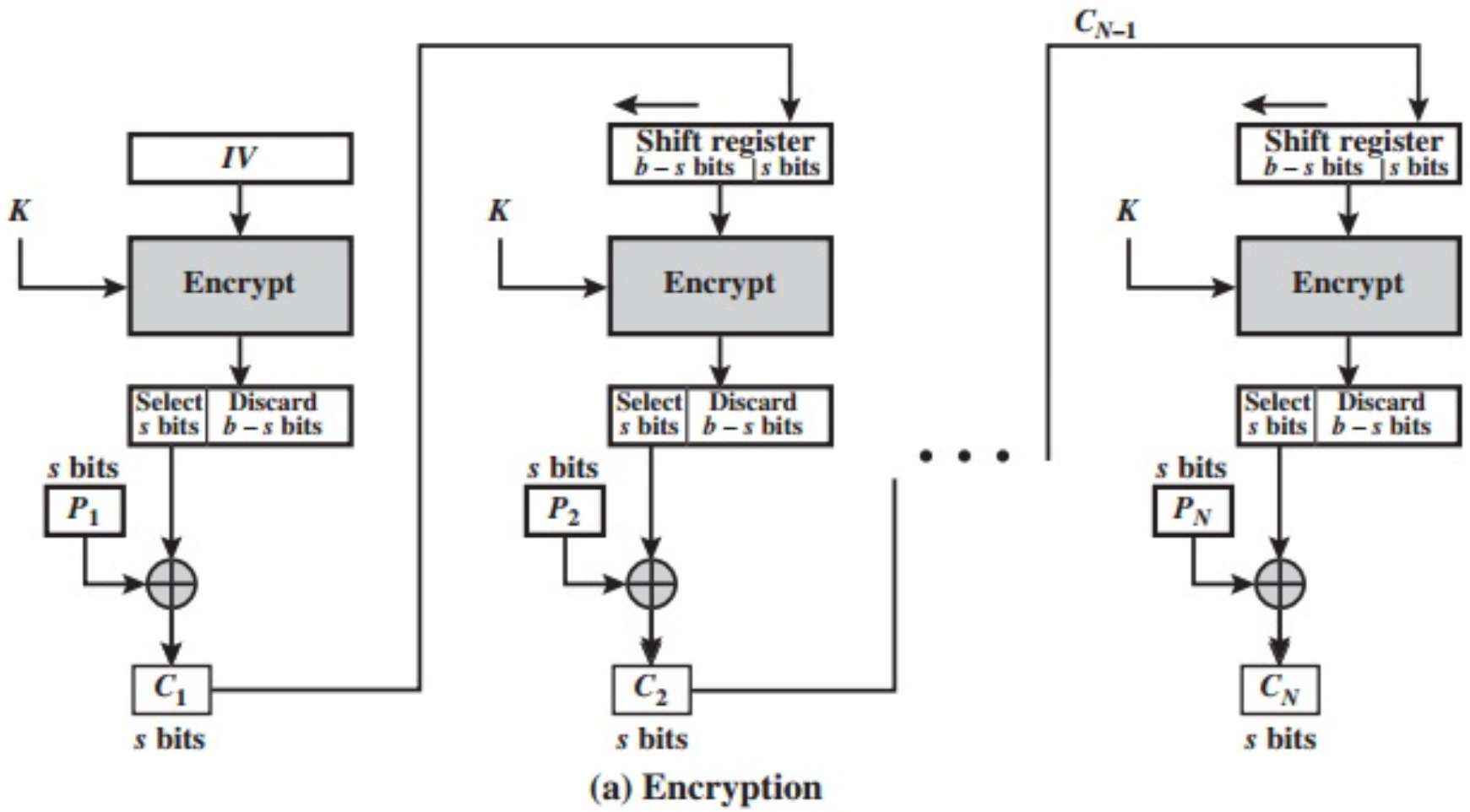



Cipher Block Chaining (CBC) mode decryption

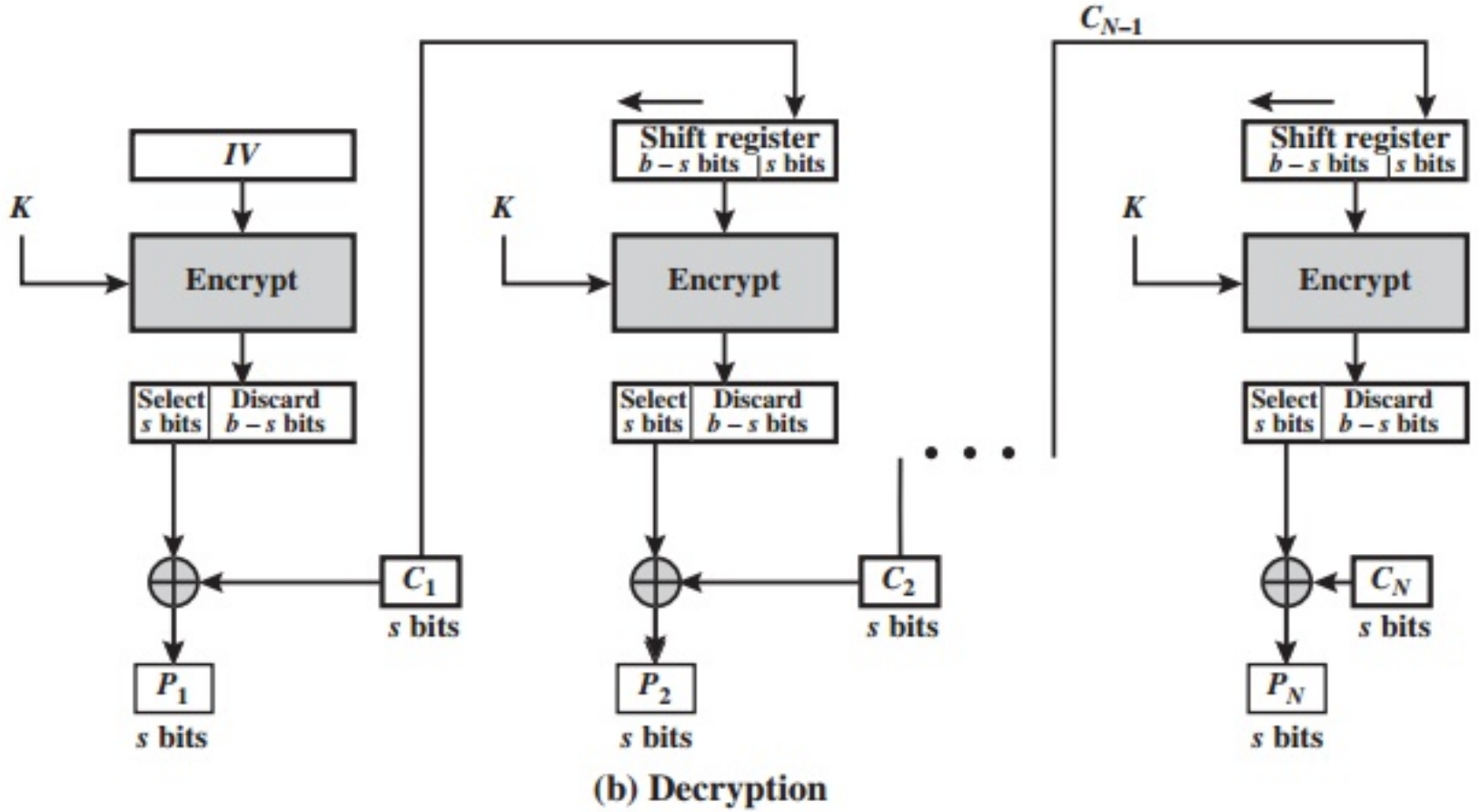
# Режим шифрования CBC. Свойства

- 1 ошибка в шифртексте ведет к неверному расшифрованию данного блока и одной ошибке при расшифровании следующего блока. На другие блоки расшифрованного текста ошибка не распространяется
- Нет стойкости к ошибкам синхронизации
- IV (Initialization Vector) может передаваться в открытом виде, но должен меняться от сообщения к сообщению

# Режим шифрования CFB-s. Зашифрование



# Режим шифрования CFB-m. Расшифрование

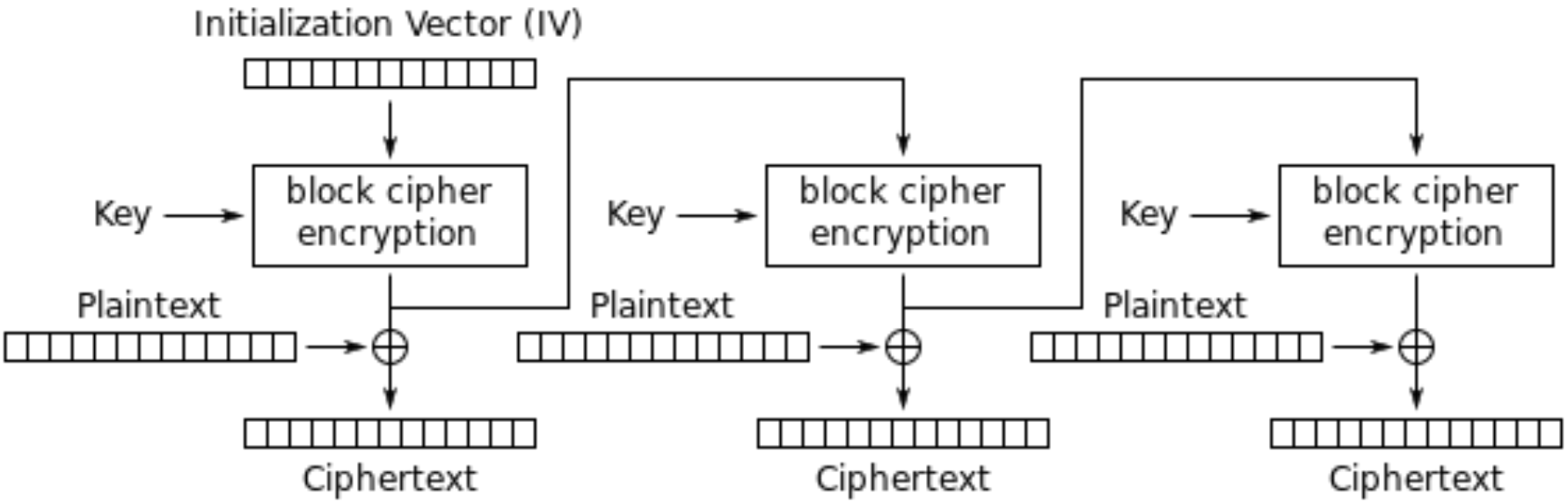



(b) Decryption

# Режим шифрования CFB-s. Свойства

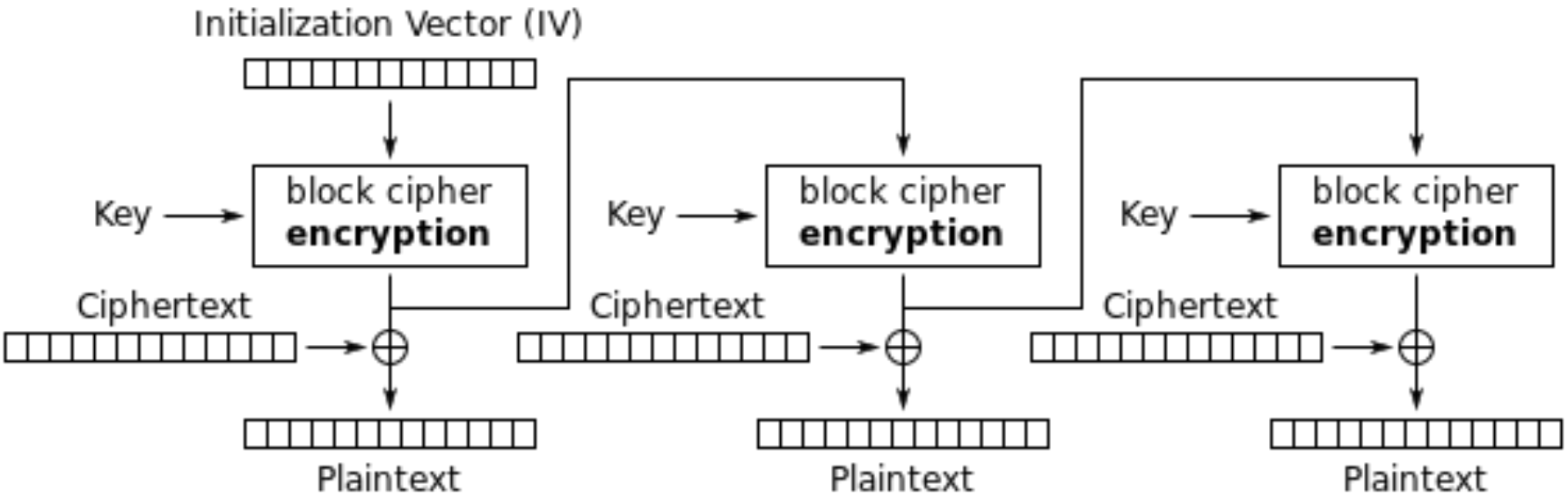
- По сути – поточный шифр
- 1 ошибка в шифртексте ведет к неверному расшифрованию нескольких блоков
- Стоек к ошибкам синхронизации
- Не требуется реализация расшифрования
- IV (Initialization Vector) может передаваться в открытом виде, но должен меняться от сообщения к сообщению
- Не требуется согласование вектора инициализации

# Режим шифрования OFB-s. Зашифрование




Output Feedback (OFB) mode encryption

# Режим шифрования OFB-s. Расшифрование




Output Feedback (OFB) mode decryption

# Режим шифрования OFB-s. Свойства

- По сути – поточный шифр
- 1 ошибка в шифртексте ведет к 1 ошибке в расшифрованном тексте
- Не стоек к ошибкам синхронизации
- Не требуется реализация расшифрования
- IV (Initialization Vector) может передаваться в открытом виде, но должен меняться от сообщения к сообщению